# wazuh

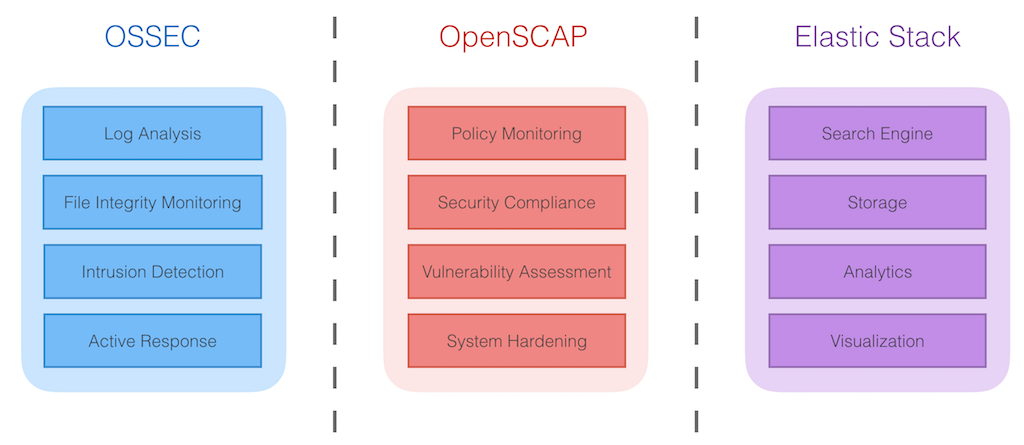
https://documentation.wazuh.com/current/getting-started/index.html

* [Docs](https://documentation.wazuh.com/current/index.html) »

* Getting started
* [Edit on GitHub](https://github.com/wazuh/wazuh-documentation/blob/3.3/source/getting-started/index.rst)

Getting started

Wazuh is a security detection, visibility, and compliance open source project. It was born as a fork of OSSEC HIDS, and later was integrated with Elastic Stack and OpenSCAP, evolving into a more comprehensive solution. Below is a brief description of these tools and what they do:

[](https://documentation.wazuh.com/current/_images/ossec_openscap_elastic_1024x4451.png)

**OSSEC HIDS**

[OSSEC HIDS](http://ossec.github.io/) is a Host-based Intrusion Detection System (HIDS) used for security detection, visibility, and compliance monitoring. It’s based on a multi-platform agent that forwards system data (e.g log messages, file hashes, and detected anomalies) to a central manager, where it is further analyzed and processed, resulting in security alerts. Agents convey event data to the central manager for analysis via a secure and authenticated channel.

Additionally, OSSEC HIDS provide a centralized syslog server and an agentless configuration monitoring system that provide security insight into the events and changes on agentless devices such as firewalls, switches, routers, access points, network appliances, etc.

**OpenSCAP**

[OpenSCAP](https://www.open-scap.org/) is an [OVAL](https://oval.mitre.org/) (Open Vulnerability Assessment Language) and [XCCDF](https://scap.nist.gov/specifications/xccdf/) (Extensible Configuration Checklist Description Format) interpreter used to check system configurations and to detect vulnerable applications.

It’s a well-known tool designed to check the security compliance and hardening of systems using industry standard security baselines for enterprise environments.

**Elastic Stack**

[Elastic Stack](https://www.elastic.co/) is a software suite (Filebeat, Logstash, Elasticsearch, Kibana) used to collect, parse, index, store, search, and present log data. It provides a web front-end that gives a high-level dashboard view of events that allows for advanced analytics and data mining deep into your store of event data.

**Table of Contents**

This document will help you understand Wazuh’s components and architecture, and will show you some common use cases.

* [Components](https://documentation.wazuh.com/current/getting-started/components.html)
  + [Wazuh agent](https://documentation.wazuh.com/current/getting-started/components.html#wazuh-agent)
  + [Wazuh server](https://documentation.wazuh.com/current/getting-started/components.html#wazuh-server)
  + [Elastic Stack](https://documentation.wazuh.com/current/getting-started/components.html#elastic-stack)
* [Architecture](https://documentation.wazuh.com/current/getting-started/architecture.html)
  + [Communications and data flow](https://documentation.wazuh.com/current/getting-started/architecture.html#communications-and-data-flow)
  + [Archival data storage](https://documentation.wazuh.com/current/getting-started/architecture.html#archival-data-storage)
* [Use cases](https://documentation.wazuh.com/current/getting-started/use-cases.html)
  + [Signature-based log analysis](https://documentation.wazuh.com/current/getting-started/use-cases.html#signature-based-log-analysis)
  + [File integrity monitoring](https://documentation.wazuh.com/current/getting-started/use-cases.html#file-integrity-monitoring)
  + [Rootkits detection](https://documentation.wazuh.com/current/getting-started/use-cases.html#rootkits-detection)
  + [Security policy monitoring](https://documentation.wazuh.com/current/getting-started/use-cases.html#security-policy-monitoring)